Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; PLUR=YES; OP=ADJ		
L4	L2 and (access$ adj2 control$)	6	L4
L3	L2 and ((role or rule or provision$) adj 2 base$)	0	L3
L2	L1 and (resource$ adj1 provider$)	38	L2
L1	(707/$ OR 705/$ OR 709/$).CCLS.	31831	L1

END OF SEARCH HISTORY

shared resource access control.

centralized resources in resource provider access control.

WEST

Generate Collection | Print

Search Results - Record(s) 1 through 6 of 6 returned.

☐ 1. Document ID: US 6460082 B1

L4: Entry 1 of 6 File: USPT Oct 1, 2002

DOCUMENT-IDENTIFIER: US 6460082 B1
TITLE: Management of service-oriented resources across heterogeneous media servers using homogenous service units and service signatures to configure the media servers

Brief Summary Text (26):
It is also an object of the present invention to allow the meta-resource to remain autonomous. Thus, according to the principles of the invention, by providing application-level access control onto a meta-resource, the autonomy of meta-resources is preserved. To this end, each service unit is associated with metadata referred to as a "service signature" which is implemented to customize the service commitment of a meta-resource, e.g., by delivering hints to the meta-resource about resource management. For example, the service signature could be used to define access rights and characteristics for any particular service unit. Similarly, the service signature may recommend run-time compensation strategies to be used to update the resource envelope for this service unit under this meta-resource type at different loads. Thus, the service signature is one of the ways in which the present invention allows the integration of service management with resource management.

Detailed Description Text (15):
Similarly, a skilled artisan will appreciate that the meta-resource needs to be trusted by the remote authority and vice-versa. Security when accessing a meta-resource is important to the content subscriber. A mechanism is needed to enforce trust between the different parties. According to today's best practices, a key-exchange mechanism such as RSA may be used to handshake with a resource provider and authenticate the resource provider. Such mechanism is applicable to any other party. Security about the content being accessed is additionally important to the content provider. Thus, enforcement of copyrights and other forms of intellectual property protection over content is necessary. A skilled artisan will appreciate that this is a recognized need and means may be deployed to facilitate the enforcement of copyright between parties having different levels of trustiness. In particular, digital watermarking techniques may be used for safeguarding the copyrights of service objects.

Detailed Description Text (25):
Via access controls over capabilities and service units, the resource provider is now enabled to grant or deny access to the download of capabilities as well as the administration and configuration of its resources into service units.

Detailed Description Text (30):
FIG. 8(a) is a flow chart depicting in greater detail the process for handling a provisioning request (800). As shown in FIG. 8(a), the signaling adapter receives the provisioning request and then forwards any such request to the SUMM which then interfaces to the service unit database in order to retrieve and update resource envelopes (805). At step (810), the service unit signature for the particular requested service is compared with resources at a particular server. Specifically, when a request arrives at the meta-resource, it is necessary to determine whether the request can be serviced, i.e., if the meta-resource is capable, has the resources, is willing to, and has the necessary capability. All these decisions are

abstracted by the service unit. Therefore, a determination is made at step (815) as to whether a service unit in a meta-resource is present indicating that the server is capable of provisioning such unit, i.e., that the necessary resources are present. The presence of a service unit provides the ability to determine the willingness of the server in accepting a request. If the service unit is not present, the request fails and the process ends without fulfillment of the request. If the service unit is present, then at step (820) a determination is made as to whether the meta-resource is willing to accept the request, i.e., if the server is willing to provide the media service when criteria such as price, current service unit utilization, and access controls, for example, are considered. Specifically, after a request arrives to the meta-resource, the meta-resource must decide whether to service the request or not. Such decision is supported by the meta-data in the resource. For example, the meta-resource (i.e., the server) determines whether the requests is associated with the right access controls (permissions) to use the service/storage bins being requested. Other criteria are price/cost admissibility. For example, the request may bound cost to $4.00 for example, whereas the meta-resource is willing to provide the service at $3.00. At step (825) the process will terminate if the request is not admissible, or, will continue otherwise. At step (835) any resource envelope adjustments are made and, at step (840), the adjusted service unit is allocated. For example, a service request may request a service unit (X, Y, Z) resource units of respective resources and is currently being serviced. A second request requests (X, Y, Z). For the adjustment step (835), a heuristics database look-up is performed and a determination made as to the form of the resulting resource allocation (f(X), g(Y), h(Z)) given the class of server (meta-resource). Once the resources are determined, any extra resources can be transferred to the overflow pool (e.g., for the duration associated for the provisioning of this request). This is accomplished during step (840) as well. Then, at step (850) the resource monitors are invoked by the operating system of the provisioning meta-resource (server) to monitor actual resources utilized in the provisioning of the requested service which is provided to the client as indicated at step (855). After provisioning of the service, the process ends at step (860) and returns to process more requests at step (865). Typically, the SUMM (FIG. 7) renders all its comparisons and determinations based on the corresponding resource envelope associated with a particular request and then requests the coordination and allocation of the service unit. However, the coordination between the various resources associated with a particular service unit is provided by the coordinated resource management module (730). In turn, the coordinated resource management module interfaces with the resource management interfaces (750) provided by the operating system found on the meta-resource.

Current US Original Classification (1):
709/226

Current US Cross Reference Classification (1):
709/223

Current US Cross Reference Classification (2):
709/224

Current US Cross Reference Classification (3):
709/225

☐ 2. Document ID: US 6397336 B2

L4: Entry 2 of 6 File: USPT May 28, 2002

DOCUMENT-IDENTIFIER: US 6397336 B2
TITLE: Integrated network security access control system

Abstract Text (1):
A network resource security services control system comprises an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism monitors activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and controllably modifies one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (2):
The present invention relates in general to data processing and communication systems, and is particularly directed to a data communication security access control mechanism, that is comprised of an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicates with one or more information resources within the network. The security access control mechanism of the invention includes monitoring activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (5):
As a reduced complexity, non-limiting example, FIG. 1 diagrammatically illustrates a network user workstation 10 which is coupled via a communication link 11 to a local area network (LAN) 20 by way of a LAN interface 13. LAN interface 13 also provides access to an external network, such as a public communication services (PCS) network, including the Internet 30, that provides potential access to any network information resource (e.g., processor-accessible digital database). The local area network 20 to which user 10 is connected customarily includes one or more computer-based units, such as the illustrated workstations 21 and 22, network server 23 and printer 24, which are interconnected via a hub 25. The hub 25 is connected to the LAN interface 13, so that the end user workstation 10 may access any `local` information resource of the LAN 20. In order to connect to the external network 30, the network interface 13 may be coupled through an electronic mail gateway 32 and a modem 33, whereby a dial-up connection may be provided to an Internet connection or other global resource provider 34, through which access to any node in the overall network is achieved.

Brief Summary Text (6):
Because the network provides a potential window into any information resource linked to any of its nodes, it is customary to both wrap or embed all communications in a `security blanket` (some form of encryption) at a communication sourcing end, and to employ one or more permission (authorization and authentication) layers that must be used to gain access to another system resource (e.g., another computer). Once installed, such schemes operate as micro security systems, primarily as binary permission filters--the user is either permitted or denied access to a destination information resource, and are customarily limited to a relatively limited (and often fixed) set of access permission criteria. Now, while such schemes provide some measure of access control, they do not provide a macro perspective or control of all of the resources for which a given network security system may be configured.

Brief Summary Text (8):
In accordance with the present invention, this problem is effectively remedied by a new and improved network resource security access control mechanism that includes protection control, access control, event management and a pro-active security agent routines integrated within the communications control software resident in a data

communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network.

Brief Summary Text (9):
The protection control routine comprises cryptography algorithms and authentication mechanisms for protecting data transported over the network. The access control routine is used in conjunction with the protection control routine and includes right to access control factors, such as time of day, length of session, etc., components, with which a user's request for access and continued activity are compared to derive inputs to the event manager. The event manager is a principal control routine that is operative to monitors activity among users and resources of the network. As it monitors these events, the event manager may take action that will controllably intervene in the current network activity for a user of interest, in response to one or more relationships associated with such activity being satisfied.

Brief Summary Text (11):
The event manager may employ a separate set of policy rules that are not known to the user and serve as an additional layer of access control for enhancing the security of the network. Such policy rules are established external to the network and may include a prescribed activity intensity level associated with the number of or total length of time a resource object may communicate with another resource. In the event a policy rule is violated, the event manager may take relatively limited action, such as sourcing a query to the user to provide further authentication or other information, such as a request to the protection control routine to employ an increased level of cryptography complexity associated with a higher network usage level. On the other hand, if the security rule set employed by the event manager classifies excessive user activity as a substantial network security `threat`, it may call up the pro-active security agent routine, so as to impair the user's ability to use the network. The security rules themselves, as objects of the overall security access control system, may be modified or updated, as required to accommodate event changes, without necessarily terminating access to the network.

Detailed Description Text (2):
Before describing in detail the new and improved network resource security access control mechanism in accordance with the present invention, it should be observed that the present invention resides primarily in what is effectively a new and improved data security access control mechanism implemented as an arrangement of abstract security services. These abstract security services include protection control, access control, event management and a pro-active security agent that are integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network. The particular resources and the information they provide, per se, are not considered part of the invention.

Detailed Description Text (4):
Attention is now directed to FIG. 2, which shows a reduced complexity, non-limiting example of an information resource network 100 having a plurality of resource nodes 110, to which one or more information resource objects, such as respective computers 120 used by user's to couple to and process data transported over the network, may be coupled, and communications among which are supervised or controlled by a network resource security services control system 200. As pointed out briefly above, and as will be detailed infra, network resource security services control system 200 communicates with each of resource and communication control objects, and includes a protection control routine 220, and access control routine 230, and event manager 240 and a pro-active security agent routine 250, which interact with one another and with network resources, so as to control the ability of network users to gain access to, transmit and retrieve information with respect to any of the resources of the network.

Detailed Description Text (7):
The access control routine 230 is used in conjunction with the protection control routine 220 and includes right to access control factors, such as time of day,

length of session, etc., components, with which a user's request for access and continued activity are compared to derive inputs to the event manager.

Detailed Description Text (9):
An object is any potential participant in the system, such as a user, information resource, communication path, protection mechanism (such as a cryptography algorithm or user's authentication procedure within the protection control routine 220), an access control feature of the access control routine 230, etc.

Detailed Description Text (14):
In addition to such usage rules, the event manager 240 may also have a separate set of policy rules that are not known to the user and serve as an additional layer of access control for enhancing the security of the network. Such policy rules may include a prescribed activity intensity level, which is associated with the number of or total length of time a resource object 120i is using the network to communicate with another resource object 120j. The policy rules may be based upon an a priori activity histogram for other users, with which the user/resource object 120i is expected to conform. As an example, should a resource object 120i spend considerably more time communicating with resource object 120j than established by the histogram, this anomaly would be detected as a violation of policy rules and cause the event manager 240 to execute one or more responses that at least temporarily intrude into the user's network/resource object access session.

Detailed Description Text (17):
Moreover, the security rules themselves, being components or objects of the overall security access control system, may be modified or updated, as required to accommodate event changes, without necessarily terminating access to the network. Thus, in the above example of user activity that might otherwise be initially perceived as exhibiting a substantial network/resource security threat, depending upon the user's interactive response, the policy rules may allow for an adjustment to the threat threshold, before permitting or discontinuing further network access. That fact that each of the security system components is tied together through the events manager substantially facilitates integrating the security services control system into the communication control software of any size or type of data communication network.

Detailed Description Text (18):
As will be appreciated from the foregoing description, the network resource security services control system of the present invention provides an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. This security access control mechanism includes monitoring activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Detailed Description Text (23):
a: Access Control

Detailed Description Text (26):
Access Control Lists (ACLs) are used by the SP to determine which clients of a secured capability are, in fact, permitted to utilize that capability.

Current US Cross Reference Classification (1):
709/229

CLAIMS:

3. The method according to claim 1, wherein step (c) comprises monitoring information generated by events associated with said user's being selectively granted access to said resource in step (b), and wherein step (d) comprises, in

response to information generated by said events satisfying a predetermined relationship with respect to access control criteria governing access to and use of said information network, diminishing the ability of said user to access a network resource.

4. The method according to claim 1, wherein said security relationships among said users and resources of said information network include a protection control routine containing a plurality of cryptography operators and authentication mechanisms for protecting data transported over said network, an access control routine including control factors associated with a right to access said network, and an event manager which monitors activity among said users and resources of said network, and wherein step (d) comprises modifying one or more of said security relationships in dependence upon one or more characteristics of said activity monitored by said event manager, so as to increase the difficulty of said user to access a network resource.

8. The mechanism according to claim 6, wherein step (b) comprises monitoring information generated by events associated with said user being selectively granted access to said resource in step (a) and, wherein step (c) comprises, in response to information generated by said events satisfying a predetermined relationship with respect to access control criteria governing access to and use of said information network, diminishing the ability of said user to access a network resource.

9. The mechanism according to claim 6, wherein said security relationships among said users and resources of said information network include a protection control routine containing a plurality of cryptography operators and authentication mechanisms for protecting data transported over said network, an access control routine including control factors associated with a right to access said network, and an event manager which monitors activity among said users and resources of said network, and wherein step (c) comprises modifying one or more of said security relationships in dependence upon one or more characteristics of said activity monitored by said event manager, so as to increase the difficulty of said user to access a network resource.

☐ 3. Document ID: US 6237023 B1

L4: Entry 3 of 6 File: USPT May 22, 2001

DOCUMENT-IDENTIFIER: US 6237023 B1
**** See image for Certificate of Correction ****
TITLE: System for controlling the authority of a terminal capable of simultaneously operating a plurality of client softwares which transmit service requests

Brief Summary Text (2):
This invention relates to an access control system and method, particular access control of a distributed system in which the resources of remote sites are shared using a computer network, by way of example.

Brief Summary Text (3):
Access control in a distributed system generally is achieved by combining an authentication mechanism in the distributed system with a resource protection mechanism at each site. For example, a distributed file system, which is a means of sharing files via a network, is used in a comparatively small-scale network environment such as a local area network (LAN). In such case user authentication means at the site level is appropriated in the network environment as well by

unifying modes of user management, and resource protection is achieved based upon the authority granted to authenticated users. The file access control means for implementing this generally is provided by the operating system (OS).

Brief Summary Text (6):
The first problem is that satisfactory reliability cannot be assured merely by applying the site-level user authentication mechanism to a distributed system. Even if modes of user management are unified between sites, no legal force is involved and a certain site is capable of individually altering some of the management information. In cases such as these, it is possible for a site administrator to impersonate a user and it is difficult for the resource provider to detect this.

Brief Summary Text (9):
Accordingly, an object of the present invention is to provide an access control system and method in which, when shared resources in a distributed system are accessed, the shared resources can be protected safely and flexibly.

Brief Summary Text (10):
According to the present invention, the foregoing object is attained by providing an access control system for controlling access to a distributed system in which resources of remote sites are shared using a computer network, comprising acquisition means for acquiring an identifier of a terminal-which requests a service and an identifier of a user, decision means for uniquely deciding authority over the service request based upon the terminal identifier and user identifier that have been acquired, and judging means for judging, using the authority that has been decided, whether or not to accept the service request.

Brief Summary Text (11):
In another aspect of the invention, the foregoing object is attained by providing an access control system for controlling access to a distributed system in which resources of remote sites are shared using a computer network, comprising relay means for acquiring an identifier of a user requesting a service, intercepting the service request by transmitting, to a prescribed address, a service request message onto which the acquired user identifier has been added, and distributing a received message, and service providing means for acquiring as a user identifier an identifier added onto the received service request message, acquiring as a terminal identifier an identifier of the relay means that transmitted this service request message, uniquely deciding authority over the service request based upon the terminal identifier and user identifier that have been acquired, and judging, using the authority that has been decided, whether or not to accept the service request.

Brief Summary Text (12):
According to the present invention, the foregoing object is attained by providing an access control method for controlling access to a distributed system in which resources of remote sites are shared using a computer network, comprising an acquisition step of acquiring an identifier of a terminal which requests a service and an identifier of a user, a decision step of uniquely deciding authority over the service request based upon the terminal identifier and user identifier that have been acquired, and a judging step of judging, using the authority that has been decided, whether or not to accept the service request.

Brief Summary Text (13):
In another aspect of the invention, the foregoing object is attained by providing an access control method for controlling access to a distributed system in which resources of remote sites are shared using a computer network, comprising, in relay means for intercepting a service request and distributing a received message, a first acquisition step of acquiring an identifier of a user requesting a service and a transmission step of transmitting, to service providing means, a service request message to which the acquired user identifier has been added on, and, in the service providing means, a receiving step of receiving a service request message, a second acquisition step of acquiring as a user identifier the identifier added onto the received service request message, and acquiring is a terminal identifier an identifier of the relay means that transmitted this service request message, a decision step of uniquely deciding authority over the service request based upon the terminal identifier and user identifier that have been acquired, and a judging step

of judging, using the authority that has been decided, whether or not to accept the service request.

Brief Summary Text (14):
In accordance with the present invention having the configuration described above, it is possible to provide an access control system and method in which, when shared resources in a distributed system are accessed, the shared resources can be protected safely and flexibly.

Detailed Description Text (2):
An access control system according to embodiments of the present invention will be described in detail with reference to the drawings.

Detailed Description Text (20):
Thus, in accordance with this embodiment, objects which determine whether authority is given or not can be aggregated in arbitrary units. This makes it possible to establish access control in highly flexible fashion.

Detailed Description Text (23):
An access control system according to a second embodiment of the present invention will now be described. In the second embodiment, elements substantially the same as those of the first embodiment are designated by like reference characters and need not be described again.

Detailed Description Text (30):
An access control system according to a third embodiment of the present invention will now be described. In the third embodiment, elements substantially the same as those of the first embodiment are designated by like reference characters and need not be described again.

Detailed Description Text (43):
An access control system according to a fourth embodiment of the present invention will now be described. In the fourth embodiment, elements substantially the same as those of the first embodiment are designated by like reference characters and need not be described again.

Current US Original Classification (1):
709/203

Current US Cross Reference Classification (1):
709/201

☐ 4. Document ID: US 6189104 B1

L4: Entry 4 of 6 File: USPT Feb 13, 2001

DOCUMENT-IDENTIFIER: US 6189104 B1
TITLE: Integrated network security access control system

Abstract Text (1):
A network resource security services control system comprises an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism monitors activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and controllably modifies one or more security relationships of a security association

that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (2):
The present invention relates in general to data processing and communication systems, and is particularly directed to a data communication security access control mechanism, that is comprised of an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. The security access control mechanism of the invention includes monitoring activity associated with a user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Brief Summary Text (5):
As a reduced complexity, non-limiting example, FIG. 1 diagrammatically illustrates a network user workstation 10 which is coupled via a communication link 11 to a local area network (LAN) 20 by way of a LAN interface 13. LAN interface 13 also provides access to an external network, such as a public communication services (PCS) network, including the Internet 30, that provides potential access to any network information resource (e.g., processor-accessible digital database). The local area network 20 to which user 10 is connected customarily includes one or more computer-based units, such as the illustrated workstations 21 and 22, network server 23 and printer 24, which are interconnected via a hub 25. The hub 25 is connected to the LAN interface 13, so that the end user workstation 10 may access any `local` information resource of the LAN 20. In order to connect to the external network 30, the network interface 13 may be coupled through an electronic mail gateway 32 and a modem 33, whereby a dial-up connection may be provided to an Internet connection or other global resource provider 34, through which access to any node in the overall network is achieved.

Brief Summary Text (6):
Because the network provides a potential window into any information resource linked to any of its nodes, it is customary to both wrap or embed all communications in a `security blanket` (some form of encryption) at a communication sourcing end, and to employ one or more permission (authorization and authentication) layers that must be used to gain access to another system resource (e.g., another computer). Once installed, such schemes operate as micro security systems, primarily as binary permission filters--the user is either permitted or denied access to a destination information resource, and are customarily limited to a relatively limited (and often fixed) set of access permission criteria. Now, while such schemes provide some measure of access control, they do not provide a macro perspective or control of all of the resources for which a given network security system may be configured.

Brief Summary Text (8):
In accordance with the present invention, this problem is effectively remedied by a new and improved network resource security access control mechanism that includes protection control, access control, event management and a pro-active security agent routines integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network.

Brief Summary Text (9):
The protection control routine comprises cryptography algorithms and authentication mechanisms for protecting data transported over the network. The access control routine is used in conjunction with the protection control routine and includes right to access control factors, such as time of day, length of session, etc., components, with which a user's request for access and continued activity are

compared to derive inputs to the event manager. The event manager is a principal control routine that is operative to monitors activity among users and resources of the network. As it monitors these events, the event manager may take action that will controllably intervene in the current network activity for a user of interest, in response to one or more relationships associated with such activity being satisfied.

Brief Summary Text (11):
The event manager may employ a separate set of policy rules that are not known to the user and serve as an additional layer of access control for enhancing the security of the network. Such policy rules are established external to the network and may include a prescribed activity intensity level associated with the number of or total length of time a resource object may communicate with another resource. In the event a policy rule is violated, the event manager may take relatively limited action, such as sourcing a query to the user to provide further authentication or other information, such as a request to the protection control routine to employ an increased level of cryptography complexity associated with a higher network usage level. On the other hand, if the security rule set employed by the event manager classifies excessive user activity as a substantial network security `threat`, it may call up the pro-active security agent routine, so as to impair the user's ability to use the network. The security rules themselves, as objects of the overall security access control system, may be modified or updated, as required to accommodate event changes, without necessarily terminating access to the network.

Detailed Description Text (2):
Before describing in detail the new and improved network resource security access control mechanism in accordance with the present invention, it should be observed that the present invention resides primarily in what is effectively a new and improved data security access control mechanism implemented as an arrangement of abstract security services. These abstract security services include protection control, access control, event management and a pro-active security agent that are integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network. The particular resources and the information they provide, per se, are not considered part of the invention.

Detailed Description Text (4):
Attention is now directed to FIG. 2, which shows a reduced complexity, non-limiting example of an information resource network 100 having a plurality of resource nodes 110, to which one or more information resource objects, such as respective computers 120 used by user's to couple to and process data transported over the network, may be coupled, and communications among which are supervised or controlled by a network resource security services control system 200. As pointed out briefly above, and as will be detailed infra, network resource security services control system 200 communicates with each of resource and communication control objects, and includes a protection control routine 220, and access control routine 230, and event manager 240 and a pro-active security agent routine 250, which interact with one another and with network resources, so as to control the ability of network users to gain access to, transmit and retrieve information with respect to any of the resources of the network.

Detailed Description Text (7):
The access control routine 230 is used in conjunction with the protection control routine 220 and includes right to access control factors, such as time of day, length of session, etc., components, with which a user's request for access and continued activity are compared to derive inputs to the event manager.

Detailed Description Text (8):
The event manager 240 is a routine that monitors network activity, in particular `events` occurring as a result of activity among users and resources of the network. An event is an activity that occurs when a user executes activity in the network, or as a result of exercising or using a resource or object within the system. An object is any potential participant in the system, such as a user, information resource, communication path, protection mechanism (such as a cryptography algorithm or user's

authentication procedure within the protection control routine 220), an access control feature of the access control routine 230, etc.

Detailed Description Text (13):
In addition to such usage rules, the event manager 240 may also have a separate set of policy rules that are not known to the user and serve as an additional layer of access control for enhancing the security of the network. Such policy rules may include a prescribed activity intensity level, which is associated with the number of or total length of time a resource object 120i is using the network to communicate with another resource object 120j. The policy rules may be based upon an a priori activity histogram for other users, with which the user/resource object 120i is expected to conform. As an example, should a resource object 120i spend considerably more time communicating with resource object 120j than established by the histogram, this anomaly would be detected as a violation of policy rules and cause the event manager 240 to execute one or more responses that at least temporarily intrude into the user's network/resource object access session.

Detailed Description Text (16):
Moreover, the security rules themselves, being components or objects of the overall security access control system, may be modified or updated, as required to accommodate event changes, without necessarily terminating access to the network. Thus, in the above example of user activity that might otherwise be initially perceived as exhibiting a substantial network/resource security threat, depending upon the user's interactive response, the policy rules may allow for an adjustment to the threat threshold, before permitting or discontinuing further network access. That fact that each of the security system components is tied together through the events manager substantially facilitates integrating the security services control system into the communication control software of any size or type of data communication network.

Detailed Description Text (17):
As will be appreciated from the foregoing description, the network resource security services control system of the present invention provides an integrated arrangement of security services, that are operative to control the ability of an information storage and retrieval network user to have access to and communicate with one or more information resources within the network. This security access control mechanism includes monitoring activity associated with user's attempt to and actual conducting of data communications with respect to a system resource, and also the controllable modification of one or more security relationships of a security association that has been established among the users and resources of the system, in dependence upon one or more characteristics of the monitored activity, in such a manner that affects the ability of the system user to conduct data communications with respect to a system resource.

Current US Cross Reference Classification (1):
709/229

CLAIMS:

5. A method according to claim 1, wherein step (c) comprises monitoring information generated by a plurality of events associated with said network user's accessing said network resource in step (b), and wherein step (d) comprises, in response to information generated by said plurality of events satisfying a predetermined relationship with respect to access control criteria governing access to and use of said information network, decreasing the ability of said network user to access a network resource.

6. A method of controlling the ability of a user to access one or more information resources of an information network comprising the steps of:

(a) providing a protection control routine having a plurality of cryptography operators and authentication mechanisms for protecting data transported over said network, an access control routine including control factors associated with a right to access said network, and an event manager which monitors activity among users and resources of said network;

(b) selectively permitting a user to access a network resource in accordance with at least one of a plurality of security relationships among users and resources of said information network; and

(c) controllably modifying one or more of said plurality of security relationships in dependence upon one or more characteristics of said activity monitored by said event manager, so as to affect the ability of said user to access a network resource.

☐ 5. Document ID: US 5742772 A

L4: Entry 5 of 6 File: USPT Apr 21, 1998

DOCUMENT-IDENTIFIER: US 5742772 A
TITLE: Resource management system for a broadband multipoint bridge

Detailed Description Text (17):
7. access control policy (e.g., open, restricted client list)

Detailed Description Text (38):
In general terms, a QOS contract is an agreement with a resource provider for use of that resource to satisfy a specific performance requirement. QOS defines the expected performance for data transport on a flow. It is specified as a set of parameters describing the type of QOS contract, traffic and performance. Broadband networks are designed to support QOS contracts on an end to end basis. In the system of the present invention, these contracts are extended to encompass bridge operation.

Current US Original Classification (1):
709/226

Current US Cross Reference Classification (3):
709/229

Current US Cross Reference Classification (4):
709/240

☐ 6. Document ID: US 5649196 A

L4: Entry 6 of 6 File: USPT Jul 15, 1997

DOCUMENT-IDENTIFIER: US 5649196 A
TITLE: System and method for distributed storage management on networked computer systems using binary object identifiers

Detailed Description Text (16):
Program control then continues with step 132 where the Distributed Storage Manager

program 24 separates the file identified by the Backup Queue Record 75 currently being processed into its component data streams. Each data stream is then processed individually. Those of ordinary skill in the art will recognize that these data streams may represent regular data, extended attribute data, access control list data, etc. Program control continues with step 134 where the Distributed Storage Manager program 24 determines whether each of the data streams currently being processed is larger than the maximum binary object size (currently one (1) megabyte). If the data stream is larger than one (1) megabyte, program control continues with step 136 where the data stream currently being processed is segmented into multiple binary objects smaller in size than one (1) megabyte. Either following step 136 or, if the determination is made in step 134 that the data stream currently being processed is not larger than one (1) megabyte (and, thus, the data stream is represented by a single binary object), program control continues with step 138.

Detailed Description Text (31):
The Resource Allocation Routine performed by the Distributed Storage Manager program 24 of the present invention is depicted in the flow chart of FIG. 5f. The Resource Allocation Routine is a process that responds to messages from other routines of the Distributed Storage Manager program 24 and allocates resources between resource requesters and resource providers. Program control begins with step 332 where the Resource Allocation Routine executed by the Distributed Storage Manager program 24 waits for a message from a Distributed Storage Manager program 24 routine. When a message is received, program control continues with step 334 where the Resource Allocation Routine determines whether the message is from a Backup/Restore Routine transmitting information relating to its highest priority binary object for compression. If such a message is received, program control continues with step 336 where the Resource Allocation Routine stores this information in an internal table containing Backup/Restore Routine status information. The Resource Allocation Routine then scans this status information table to ascertain which Backup/Restore Routine has the highest priority binary object for storage. Program control then continues with step 338 where the Resource Allocation Routine determines whether any Compression Routine is available to process the highest priority binary object. If no Compression Routine is available for processing, program control is returned to step 332. If an available Compression Routine is located, program control continues with step 340 where the Resource Allocation Routine transmits a message to the requesting Backup/Restore Routine indicating which Compression Routine is available to compress the binary object. In addition, the Resource Allocation Routine marks the Compression Routine as "working" in an internal table containing Compression Routine information. Program control is then returned to step 332.

Current US Original Classification (1):
707/204

Current US Cross Reference Classification (1):
707/202

Current US Cross Reference Classification (2):
707/9

Term	Documents
ACCESS$	0
ACCESS	463265
ACCESSA	1
ACCESSABILE	1
ACCESSABILITY	1182
ACCESSABILITY-INADVERTENT	1
ACCESSABILITY/MAINTAINABILITY	1
ACCESSABILTY	1
ACCESSABLE	2045
ACCESSABLEMEMORY	3
ACCESSABLY	17
(L2 AND (ACCESS$ ADJ2 CONTROL$)).USPT.	6

There are more results than shown above. Click here to view the entire set.

Display Format: KWIC Change Format

Previous Page Next Page